Mission Assurance Guidelines

Presentation to GSFC Code 300

03/18/2003

Sam Archer-Davies

Agenda

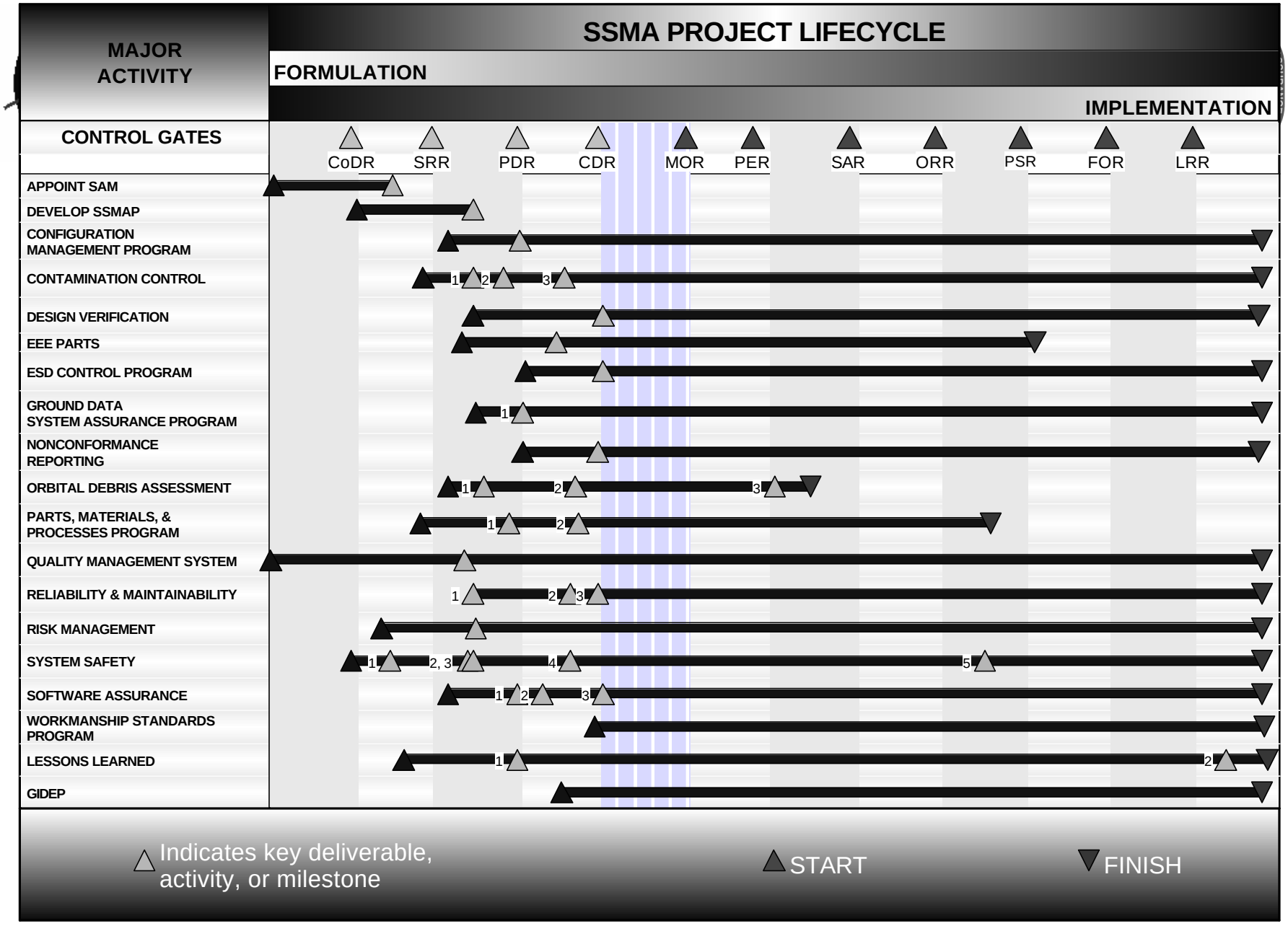
- Introduction/Overview of 7120 Documentation
  - 300-PG-7120.2.1
  - 300-PG-7120.2.2
- MAG Usage
- MAG Attributes
- MAG Contents
- Rewrite of Software Quality Assurance
- Issues/Concerns/Limitations
- Maintenance Process Overview
- Candidate Process Improvements/Future Revs.
- Conclusion

7120 Documentation

- GPG 7120.2.2 Project Management
- 300-PG-7120.2.1 MAG Implementation
  - Guidance on establishing a SSMAP and content of a SSMAP
  - Brief 4 pages
- 300-PG-7120.2.2 MAG for Tailoring the needs for GSFC Projects
  - Laundry list of various disciplines
  - Exhaustive 147 pages

300-PG-7120.2.1

- **Who**
  - SAM assigned to Project
  - SAM works w/Project to develop SSMAP that is tailored to mission requirements, characteristics, etc
- **What (Content of SSMAP)**
  - QMS compliant with ISO 9001 or equivalent
  - System Safety Program (see GPG 8700.2)
  - Reliability and Maintainability Program (see GPG 8700.1)
  - SW Assurance Program
  - Ground Data Assurance Program
  - Risk Management Program (see GPG 7120.2)
  - Technical Review Program (see GPG 8700.4)
  - Design Verification Program (GPG 8700.3)
  - Workmanship Stds (see GPG 8700.1)
  - Parts, Materials, and Processes (see GPG 8700.2)
  - Electrostatic Discharge Control Program
  - GIDEP Participation Plan


MAJOR ACTIVITY
SSMA PROJECT LIFECYCLE
FORMULATION
IMPLEMENTATION
CONTROL GATES
CoDR
SRR
PDR
CDR
MOR
PER
SAR
ORR
PSR
FOR
LRR
APPOINT SAM
DEVELOP SSMAP
CONFIGURATION MANAGEMENT PROGRAM
CONTAMINATION CONTROL
DESIGN VERIFICATION
EEE PARTS
ESD CONTROL PROGRAM
GROUND DATA SYSTEM ASSURANCE PROGRAM
NONCONFORMANCE REPORTING
ORBITAL DEBRIS ASSESSMENT
PARTS, MATERIALS, & PROCESSES PROGRAM
QUALITY MANAGEMENT SYSTEM
RELIABILITY & MAINTAINABILITY
RISK MANAGEMENT
SYSTEM SAFETY
SOFTWARE ASSURANCE
WORKMANSHIP STANDARDS PROGRAM
LESSONS LEARNED
GIDEP
Indicates key deliverable, activity, or milestone
START
FINISH

300-PG-7120.2.2

- What
  - Detailed description of each discipline
  - Processes involved
  - Products/Key Deliverables
  - DIDs
  - Applicable Standards and Documentation
- Questionable as to whether it provides tailoring information for GSFC Projects
  - SSMA Handbook Vol. 2 will provide guidelines for tailoring
  - New NPG – “Risk Classification for NASA Payloads” will allow mapping of MAG requirements to project risk classifications - similar to SPAR

MAG Usage

- Primary Uses
  - Developing a SSMAP and ultimately a MAR
  - MAR may be placed or referenced in contract SOW
- Secondary Uses
  - General Training Resource for Code 300 personnel
  - Planning of resources
  - Basis for audits/assessments
- When
  - Throughout entire lifecycle, but primarily in Formulation Phase

MAG - Attributes

- Written with requirements that can be lifted.
- Lead-ins in most chapters are italicized to indicate editorial comments and not requirements. All editorial comments are italicized.
- Parts Requirements and Materials, Processes and Lubrication Requirements combined into Parts, Processes and Materials (PMP) Requirements.
- Electronic Packaging and Processes Requirements now in Workmanship Standards.
- Both ANSI/ISO/ASQ Q9001-1994 and ANSI/ISO/ASQ Q9001-2000 are valid through December 13, 2003, therefore, ANSI/ISO/ASQ Q9001 is used in the MAG.

MAG Contents

MAG Structure:

- Chapter 1 Overall Requirements
- Chapter 2 Quality Management System
- Chapter 3 System Safety Requirements
- Chapter 4 Reliability and Maintainability Requirements
- Chapter 5 Software Assurance Requirements
- Chapter 6 Ground Data Systems Assurance Requirements
- Chapter 7 Risk Management Requirements
- Chapter 8 Technical. Review Requirements
- Chapter 9 Design Verification Requirements
- Chapter 10 Workmanship Standards
- Chapter 11 Parts, Materials and Processes Requirements
- Chapter 12 Contamination Control Requirements
- Chapter 13 Electrostatic Discharge (ESD) Control
- Chapter 14 GIDEP Alerts and Problem Advisories

MAG Contents

- *Chapter 2 Quality Management System (QMS)*
  - QMS that is ISO compliant
  - Includes augmentations to ISO requirements
- *Chapter 3 System Safety Requirements*
  - Mandatory contract element placed directly into the contract SOW
  - System Safety Program Plan (SSPP) - describes activities of system safety management and engineering
  - Compliance with EWR-127 Launch Site Safety Requirements
  - Safety Data Package (SDP), Missile System Prelaunch Safety Data Package (MSPSP), or Safety Assessment Report (SAR)
  - Initiated in the concept phase of design and continue throughout all phases of the mission

MAG Contents

- *Chapter 4 Reliability and Maintainability Requirements*
  - Reliability and Maintainability (RM) Program Plan (RMPP): describes activities that ensure RM functions are an integral part of the design and development process; how reliability assessments will be integrated with the design process and other assurance practices to maximize the probability of meeting mission success criteria.
  - Use of FMEA; FTA; PRA, Stress Analysis, etc. to ensure mission reliability.
- *Chapter 5 Software Assurance Requirements*
- *Chapter 6 Ground Data Systems Assurance Requirements*
  - Ground Data Systems (GDS) quality plan
  - GDS components may include GDS software, firmware and hardware, ground support elements (simulators, etc), COTS, databases, key parameter and test checkout software etc.

MAG Contents

- *Chapter 7 Risk Management (RM) Requirements*
  - Requirement established by the NPG 7120.5, “NASA Program and Project Management Processes and Requirements”.
  - Implementation of Continuous Risk Management System (CRMS) that provides for identification, analysis, tracking, communication, resolution, mitigation and retirement of mission risks.
  - Applies to all software and hardware products, GDS components and processes (flight and ground).

MAG Contents

- *Chapter 8 Technical. Review Requirement*
  - Series of comprehensive system-level design reviews conducted by the GSFC SRO (Code 301).
  - Reviews cover all aspects of flight and ground hardware, software, and operations for which the developer has responsibility.
    - System Requirement review (SRR)
    - Preliminary Design Review (PDR)
    - Critical Design Review (CDR)
    - Mission Operations Review (MOR)
    - Pre-Environmental Review (PER)
    - Pre-Shipment Review (PSR)
    - Flight Operations Review (FOR)
    - Launch Readiness Review (LRR)

MAG Contents

- *Chapter 9 Design Verification Requirements*
  - Verification program to meet the guidelines of General Environmental Verification Specification for STS and ELV Payloads, Subsystems and components (GEVS-SE).
- *Chapter 10 Workmanship Standards*
  - Workmanship standards that provide process and acceptance requirements for the manufacture of reliable flight and ground support hardware.
  - Workmanship Program to assure that all electronic packaging technologies, processes and workmanship activities selected and applied meet mission objectives for quality and reliability.

MAG Contents

- *Chapter 11 Parts, Materials and Processes Requirements*
  - Parts, Materials, and Processes Control Program (PMPCP) to assure that all selected items for use in flight hardware meet mission objectives for quality and reliability. PMPCP includes but not limited to:
    - Parts, Materials, & Processes Control Board (PMPCB)
    - Shelf life control plan
    - PMP vendor surveillance and audit plan
    - PMP qualification plan
    - Incoming inspection and test plan
    - Destructive Physical Analysis (DPA) plan
    - Radiation hardness assurance program plan as required
    - Corrosion prevention and control plan.
    - Contamination Prevention and Control Plan, as required.
    - Traceability control plan.
    - Project Approved Parts List (PAPL).

MAG Contents

- *Chapter 12 Contamination Control Requirements*
  - Contamination Control Plan (CCP) to establish the contamination control implementation and methods used to measure and maintain the levels of cleanliness required during each of the various phases of the project.
- *Chapter 13 Electrostatic Discharge (ESD) Control*
  - ESD Control Program to assure that all manufacturing, inspection, testing, and other processes will not compromise mission objectives for quality and reliability due to ESD events.
- *Chapter 14 GIDEP Alerts and Problem Advisories*
  - GIDEP participation in order to detect problems that affect or potentially affect the suitability of electronic parts and materials for use in GSFC products or that affect or potentially affect personnel or system safety.

Rewrite of Software Quality Assurance

- Updates made to align existing software assurance requirements with proposed updates to the NASA Software Assurance Standard
- Software Assurance broken out into 5 disciplines – SQA, Software Safety, Software Reliability, V&V, and IV&V
- Expanded sections on Software Safety and Software Reliability
- Added sections for Software Assurance Status Reporting and NASA Oversight of Software Development
- Added verbiage regarding the necessary communication between IV&V personnel and the software development team (e.g., access to documentation and corrective action to findings)

Rewrite of Software Quality Assurance (cont)

- Updated DID's for Software Development Plan, Software Quality Assurance Plan, and Software Configuration Management Plan to bring them into compliance with applicable IEEE standards

- Future Revisions
  - Mapping SA requirements to the Risk Classification for NASA Payloads and the Software Classification Scheme (currently in draft)
  - Removing redundancy between the SA section and GDS section
  - Continue to assess and update software section to be compliant with forthcoming NASA software standards as well as IEEE 12207
  - Continue to assess and improve software safety and reliability related text/material

Issues/Concerns/Limitations

- Reuse of existing/older MARs
  - These MARs may not be consistent with/up to date with contents of most recent MAG
- MARs not placed in Contract SOW
  - Lack of binding reqs (RSDO missions/providers)
- Tailoring guidelines, principles, heuristics lacking
  - NPG – “Risk Classification for NASA Payloads” will allow mapping of MAG requirements to the Risk Classification of projects
  - SSMA Handbook Vol. 2 will provide guidelines for tailoring
- Needs to be proactively maintained
  - As things change (reqs, stds, techniques, etc) the MAG needs to change
  - Time/resources to adequately address changes

Maintenance Process Overview

- Sam Archer-Davies & Renee Taylor POC for this effort
- Falls under MASC service order 1.037 which calls for
  - Planned updates every six months of 300-PG-7120.2.2
  - Civil Servant and MASC personnel support existing service order
- Process Overview
  - civil servant and contractor personnel review and disposition all comments (see next slide for process)
  - contractor personnel make “approved edits”
  - revised MAG sent out for GDMS review
  - civil servant and contractor personnel review and disposition GDMS review comments
  - final revised MAG sent to Harold Mitchell in PDF and Word format

Maintenance Process Overview

- Review comments received from various sources
  - word of mouth, emails/verbal discussions w/SMEs, weekly/monthly meetings, GDMS review, etc.
- MAG Maintenance team continues to strive to determine most appropriate method for securing MAG review comments
  - Continue to hear comments like “when is the next revision of the MAG”, “how can I get the MAG updated”, etc
- GDMS Review process requires full participation of user community
  - 49 identified reviewers, only 11 provided comments
- Resource constrained – simply cannot get every requested change implemented in a timely fashion
  - Some changes are tabled for future versions

Candidate Process Improvements/ Future Revisions

- Tailoring guidelines for projects based on characteristics - risks classification, etc (New NPG, Handbook Volume II)
  - In-house, out-of-house, international
- Rewrite of GDS requirements
- Include ITAR requirements
- Derating requirements for EEE parts
- Real-Time X-Ray requirements

Conclusions

- MAG needs to evolve & be maintained as our environment changes
- Without your support, the MAG cannot be properly maintained - we need your comments/updates!
- We want the MAG to be a valuable asset for Code 300
- Most current versions are
  - 300-PG-7120.2.1 Rev B
  - 300-PG-7120.2.2 Rev C
- Comments, Questions/Answers

Backup Chart - 1

- What is happening with the ISO Standard?
  - ISO 9001:2000 revision published December 13, 2000
  - ISO 9001:1994 “canceled”
  - Registered organizations have until December 13, 2003 to successfully transition to ISO 9001:2000 registration or face ISO de-registration

Backup Chart - 2

Wasn't the NASA ISO requirement going away?

- As a result of F2M, NPD 1280.1 was drafted, reviewed and released.
  - Does not require ISO compliance.
  - However, Centers must describe (to Deputy Administrator) management systems and method of verifying effectiveness.
    - Third party registration to ISO 9001:2000 or AS 9100 would meet the requirement
    - Third party audits must be employed in any event
    - Centers could invent their own unique management system standard that meets the minimum criteria, subject to HQ approval
- GSFC Center Director decided to continue ISO certification.

Backup Chart - 3

- Now what?
  - ISO 9001:2000 registration audit scheduled for August/September 2003
  - Schedule allows time to correct any major nonconformances before December deadline
  - Consequently, an ISO 9001:2000 compliant QMS must be in place in May 2003 to accommodate a full cycle of internal audits and the generation of at least 3 months of objective evidence